



U.S. Department of Justice

*United States Attorney
Eastern District of New York*

AFM:EHS/AA
F. #2022R00315

*271 Cadman Plaza East
Brooklyn, New York 11201*

May 28, 2025

By ECF and E-mail

The Honorable Frederic Block
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Sagar Steven Singh
Criminal Docket No. 23-CR-236 (FB)

Dear Judge Block:

The government respectfully submits this letter in advance of the defendant Sagar Steven Singh's sentencing, which is scheduled for June 4, 2025. The defendant pleaded guilty to Counts One and Two of the indictment, charging violations of 18 U.S.C. § 371 (Conspiracy to Commit Computer Intrusions) and 18 U.S.C. §§ 1028A(a)(1), (b), and (c)(4) (Aggravated Identity Theft).¹ See PSR ¶¶ 1–2. For the reasons stated below, the government respectfully requests a sentence within the Guidelines range of 30 to 36 months' imprisonment.

I. Background

A. "ViLE"

The defendant and co-defendant Nicholas Ceraolo were members of "ViLE," a cybercriminal organization. PSR ¶ 7. Members of ViLE conspired to illegally obtain victims' personal information and maliciously used it to harass, threaten, or extort victims. *Id.* ViLE's logo is a girl being hanged (PSR ¶ 10) pictured below. The defendant's nickname "Weep" appears under the picture:

¹ The information below is taken from the United States Probation Department ("Probation") Presentence Investigation Report ("PSR") dated April 30, 2025 and other evidence gathered as part of the investigation and prosecution of the defendant.



ViLE members, including the defendants, used sophisticated methods to obtain victims' personal information, including by submitting fraudulent legal process to social media companies to get user registration information. PSR ¶ 8. The defendants also co-opted and corrupted corporate insiders, searched public and private online databases, and, as charged in the instant indictment, accessed a nonpublic United States government database without authorization and unlawfully used official email accounts belonging to law enforcement officers in other countries. *Id.*

After obtaining victim information, the defendants posted it on an online forum ("Forum-1"), administered by the leader of ViLE, an unindicted co-conspirator who lives abroad. PSR ¶ 9. Victims were then extorted into paying a ransom, or surrendering access to their social media accounts, in exchange for ViLE members removing their personal information from Forum-1. *Id.*

Singh was an enthusiastic participant in ViLE. In multiple online chats, he discussed his efforts to "expand[]" and "rebrand[]" the group, and bragged about the money he was making by "doxing" targets.²

B. The Defendant Breached a Secure Government Database

In May 2022, the defendants conspired to access a nonpublic portal maintained by a United States federal law enforcement agency (the "Federal Law Enforcement Agency") without authorization, thereby obtaining confidential, restricted information. *See* PSR ¶ 11–15. Specifically, defendant Singh unlawfully used a law enforcement officer's stolen password to access the nonpublic, password-protected online portal ("the Portal") for federal law enforcement use only. *Id.* Access to the Portal was restricted to law enforcement officials. *See* PSR ¶ 11. Any user who entered the Portal had to view and click through multiple warning screens, including a

² Doxing refers to the action or process of searching for and publishing private or identifying information about a particular individual on the internet with malicious intent.

warning that “unauthorized use or access to [the] system may subject you to criminal and/or civil prosecution and penalties,” before proceeding. PSR ¶ 12.

The Portal was utilized for confidential law enforcement functions, including sharing intelligence between law enforcement agencies and maintaining nonpublic records of narcotics and currency seizures. *See* PSR ¶ 11–12. The Portal also was used for storing and maintaining law enforcement intelligence reports. PSR ¶ 11.

On May 7, 2022, Singh used a username and password belonging to a local police officer (hereinafter, “the Stolen Credentials”) to log in to the Portal without authorization. PSR ¶ 13. Singh connected to the Portal from an IP address that had, in turn, previously been used to access a social media account registered to Singh. PSR ¶ 13. Records from Singh’s computer and the Federal Law Enforcement Agency’s servers indicate that Singh accessed various portions of the Portal, including multiple guides to using the Portal and law enforcement databases that track narcotics seizures in the United States. *Id.* Singh also clicked on links within the Portal that led to other Federal Law Enforcement Agency databases; however, he was unable to access those databases because they required separate credentials. *Id.*

After gaining unauthorized access to the Portal, Singh boasted about his access to Ceraolo, and the men acknowledged that the conduct was criminal. PSR ¶ 15. Singh wrote to Ceraolo: “Im going to jail. That fucking portal I accessed I shouldn’t have been there. The shit I found on there. Im no gov official.” *See id.* In a separate conversation, Singh wrote to another individual about his breach of the Portal, stating: “That portal shit I accessed I was not supposed to be there not one bit I jacked into a police officer’s account.”

Singh used his access to the Portal to harass and extort others. On May 9, 2022, Singh circulated screenshots of text messages between himself and an individual whom Singh was extorting (hereinafter, “Victim-1”). PSR ¶ 16. In the messages, Singh sent Victim-1 an extensive set of personal details associated with Victim-1, including Victim-1’s social security number, driver’s license number, cellphone number, and home address. Singh asked: “look familiar?” *Id.* Singh told Victim-1 that he had “access to [redacted] databases, which are federal, through [the] portal, i can request information on anyone in the US doesn’t matter who, nobody is safe.” *Id.*³ Singh. Singh then advised Victim-1: “you’re gonna comply to me if you don’t want anything negative to happen to your parents ... I have every detail involving your parents ... allowing me to do whatever I desire to them in malicious ways.” *Id.* Singh demanded the credentials to Victim-1’s Instagram accounts and added: “leave the details here and I won’t harm anyone.” *Id.* During the conversation, Singh ultimately directed Victim-1 to sell Victim-1’s account credentials and send the proceeds of the sale to Singh.

Singh’s online conduct was notable for its sadistic nature. In one chat, Singh and another individual discussed threatening a video game player’s mother to force the victim to give

³ Despite this claim, it is not clear whether the details that Singh sent to Victim-1 were in fact derived from the Portal.

his or her account login information to Singh so that it could be resold for profit—much as Singh threatened Victim-1. Singh wrote: “Do we send a bomb squad for fun,” then added, “No,,,,, [sic] his mom might have a heart attack.” Singh then wrote: “Actually maybe if she had a Minor stroke.” The other individual interjected: “she will probably end up dead.” Singh wrote: “that would be beneficial[.]”

C. The Defendant Continued to Engage in Cybercrime After Law Enforcement Contact and a Search of His Residence

On September 14, 2022, Homeland Security Investigations agents executed a warrant to search Singh’s home and seized multiple electronic devices that contained evidence of cybercrimes. Six months later, on March 14, 2023, Singh was arrested at home pursuant to a warrant. The law enforcement agents conducting the arrest announced themselves at the door. Singh came to the door after a period of delay, during which the agents observed him moving from room to room inside his home. The agents entered Singh’s home and placed him in handcuffs. As they were handcuffing Singh, the agents observed a mobile phone in the microwave oven—in an apparent attempt to conceal or destroy the phone.⁴ A judicially authorized search of the phone showed that Singh had continued to engage in identity theft and computer-related fraud in 2023 following the search of his home—despite knowing that law enforcement was investigating his cybercrime activities. That evidence showed that Singh and others fraudulently obtained and exchanged highly sensitive personal and financial information—names, addresses, bank information, and social security numbers.

D. Defendant’s Sentencing Memorandum

By sentencing memorandum dated May 27, 2025, the defendant seeks a sentence no greater than the mandatory minimum of two years. Mem. 1, ECF No. 55. The memorandum details the defendant’s losses of his grandparents in 2017 and his father’s subsequent passing in 2020. Mem. 2-3. The defendant argues that the death coincided with the pandemic’s isolation, leading Singh to spend increasing time online. Mem. 3. The defendant also argues that Singh’s youth at the time of the offense warrant merits a downward variance. Mem. 4-5.

II. Applicable Law

The Supreme Court has explained that “a district court should begin all sentencing proceedings by correctly calculating the applicable the United States Sentencing Guidelines (“U.S.S.G.” and “Guidelines”) range. *Gall v. United States*, 552 U.S. 38, 49 (2007). Though advisory, *see United States v. Booker*, 543 U.S. 220, 264 (2005), the Guidelines nonetheless are “the starting point and the initial benchmark,” *Gall*, 552 U.S. at 49; *see also Molina-Martinez v. United States*, 578 U.S. 189, 198–99 (2016) (explaining that “[t]he Guidelines are the framework

⁴ As a result, Singh was later charged with obstruction of justice. *See* Indictment, Count Five. The government has agreed to seek dismissal of Count Five after sentencing in connection with the defendant’s plea to Counts One and Two of the Indictment.

for sentencing and anchor the district court's discretion" (alternation and internal quotation marks omitted)).

After calculating the applicable Guidelines range, the court must consider the factors outlined in § 3553(a), *see Gall*, 552 U.S. at 49, and impose a sentence "sufficient, but not greater than necessary to fulfill the purposes of sentencing," *United States v. Cavera*, 550 F.3d 180, 188 (2d Cir. 2008) (citing 18 U.S.C. § 3553(a)(2)). Section 3553(a) directs the court "in determining the particular sentence to impose" to evaluate: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the statutory purposes noted above; (3) the kinds of sentences available; (4) the kinds of sentence and the sentencing range as set forth in the Sentencing Guidelines; (5) the Sentencing Guidelines policy statements; (6) the need to avoid unwarranted sentencing disparities; and (7) the need to provide restitution to any victims of the offense.

Although the Guidelines are no longer mandatory, they continue to play a critical role in trying to achieve the "basic aim" that Congress sought to meet in enacting the Sentencing Reform Act, namely, "ensuring similar sentences for those who have committed similar crimes in similar ways." *Booker*, 543 U.S. at 252. "[I]n the ordinary case, the Commission's recommendation of a sentencing range will reflect a rough approximation of sentences that might achieve § 3553(a)'s objectives." *Kimbrough v. United States*, 552 U.S. 85, 109 (2007) (citation and internal quotation marks omitted). Indeed, the Supreme Court has held that, on appeal, a Guidelines sentence may be presumed to be reasonable because "the sentencing statutes envision both the sentencing judge and the [Sentencing] Commission as carrying out the same basic § 3553(a) objectives." *Rita v. United States*, 551 U.S. 338, 358 (2007). "An individual judge who imposes a sentence within the range recommended by the Guidelines thus makes a decision that is fully consistent with the Commission's judgment in general." *Id.* at 350. Furthermore, sentences within the applicable Guidelines promote Congress' goal in enacting the Sentencing Reform Act: "to diminish unwarranted sentencing disparity." *Id.* at 354.

At sentencing, "the court is virtually unfettered with respect to the information it may consider." *United States v. Alexander*, 860 F.2d 508, 513 (2d Cir. 1988). Indeed, "[n]o limitation shall be placed on the information concerning the background, character, and conduct of a person convicted of an offense which a court of the United States may receive and consider for the purpose of imposing an appropriate sentence." 18 U.S.C. § 3661.

III. Guidelines

The Guidelines calculation detailed in the PSR is incorrect as further described below. The correct Guidelines range of imprisonment is 30 to 36 months' imprisonment. Count 1 carries a 6-12 months' imprisonment Guidelines range. Count 2 carries a mandatory minimum sentence of 24 months' imprisonment.

A. The Applicable Guidelines Range

The appropriate Guidelines calculation is set forth below:

Base Offense Level (U.S.S.G. § 2X1.1 & 2B1.1(a)(2))	6
Plus: Offense Involved Sophisticated Means (U.S.S.G. § 2B1.1(b)(10)(C))	+2
Plus: Offense Involved Misrepresentation Acting on Behalf of Government (U.S.S.G. § 2B1.1(b)(9))	+2
Plus: Offense Involved Dissemination of Personal Information (U.S.S.G. § 2B1.1(b)(18))	+2
Plus: Offense Involved a Computer System Used by Government in Furtherance of the Administration of Justice (U.S.S.G. § 2B1.1(b)(19)(A)(i))	+2
Less: Adjustment for Zero-Point Offenders (U.S.S.G. § 4C1.1)	-2
Total:	<u>12</u>

The Probation Department correctly calculated the base level offense of 6 and applied the sophisticated means enhancement (PSR ¶¶ 36-37), arriving at a total offense level of 12, after application of U.S.S.G. § 2B1.1(b)(10)(C) (adjusting the offense level to 12 if it would otherwise be less than 12). PSR ¶ 37.

The government disagrees, however, with Probation's calculation of the total offense level, because it fails to account for several applicable enhancements: U.S.S.G. § 2B1.1(b)(9)(a) (Offense Involved Misrepresentation Acting on Behalf of Government); U.S.S.G. § 2B1.1(b)(18) (Offense Involved Dissemination of Personal Information); and U.S.S.G. § 2B1.1(b)(19)(A)(i) (Offense Involved a Computer System Used By Government In Furtherance of The Administration of Justice). For the reasons that follow, each of these enhancements is applicable and the Court should find that they all apply.

First, the defendant falsely represented that he was acting on behalf of a government entity. He used, without authorization, login credentials belonging to a government official to access sensitive law enforcement information in the Portal. PSR ¶ 18. Moreover, Singh and Ceraolo used an email account belonging to a Bangladeshi police official to communicate with U.S.-based social media platforms, purporting to be a police officer contacting the providers from an official police account. PSR ¶¶ 19-20. The Second Circuit has affirmed the application of § 2B1.1(b)(9)(a) where the defendant posed as law enforcement. *See United States v. Nieves*, 727 F. App'x 721, 724 (2d Cir. 2018) (affirming district court's application of § 2B1.1(b)(9)(a) where defendant misrepresented himself as a "federal immigration officer" with the power to help his

victims obtain lawful immigration status in return for payment of bribes). Accordingly, the Court should apply § 2B1.1(b)(9)(a).

Second, the offense involved dissemination of personal information. As described above, ViLE members, including the defendant and his codefendant, used various sophisticated methods to obtain victims' personal information. PSR ¶ 8. After obtaining victim information, ViLE members posted it on Forum-1 and extorted victims. Based on these facts, the Court should apply U.S.S.G. § 2B1.1(b)(18).

Third, the offense involved a computer system used by government in furtherance of the administration of justice. The term "government entity" includes the "Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country." 18 U.S.C. § 1030. Here, the government entity is the federal law enforcement agency which operates the Portal. Specifically, defendant Singh unlawfully used a law enforcement officer's stolen password to access the nonpublic Portal. Access to the Portal was restricted to law enforcement officials (PSR ¶ 11) and used for law enforcement. As such, the Court should find that U.S.S.G. § 2B1.1(b)(19)(A)(i) applies.

Assuming acceptance of responsibility, the adjusted offense level falls to 10. This carries a Guidelines range of 6 to 12 months. Because the two-year statutory minimum sentence for aggravated identity theft must run consecutively to any other counts (PSR ¶ 80; 18 U.S.C. § 1028A(b)), the defendant's total Guidelines range is 30 to 36 months' imprisonment.

IV. Defendant Objections

A. Restitution

In a letter dated May 15, 2025 ("Ltr."), the defendant objects to paragraphs 26, 91 and 92 of the PSR as they relate to the order of restitution in this case. Ltr. 1. The defendant errs in arguing that there is no victim of the offenses to which he pled guilty.

The Mandatory Victims Restitution Act ("MVRA") authorizes a sentencing court to order a defendant to pay restitution to a "victim" of the offense, and it defines "victim" as "a person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered[.]" 18 U.S.C. § 3663A(a)(2). "Where a defendant has pled guilty to an offense, we look to the materials supporting the plea—such as the allocution statement, the plea agreement, and the indictment—to ascertain the 'offense of conviction' for restitution purposes." *United States v. Goodrich*, 12 F.4th 219, 230 (2d Cir. 2021).

In this case, Count One of the Indictment, to which the defendant pled guilty, lays out the offense, including that: "On or about May 9, 2022, SINGH wrote to an individual whose identity is known to the Grand Jury (Victim-1) that SINGH had 'access to [] databases, which are federal' through which he could 'request information on anyone in the US doesn't matter who, nobody is safe.'" Indictment ¶ 6.v. Because the offense of conviction expressly references how

the defendant intended to abuse his access to the Portal to harass, intimidate and extort Victim-1, there is a victim for restitution purposes. Thus, the Court should overrule the objection.⁵

B. Supervised Release Conditions

The defendant also objects to the computer monitoring condition at paragraph 97. Ltr. 2. While the condition can be narrowed to exclude geolocation tracking, the proposed computer monitoring is an otherwise appropriate condition of supervised release.

“District courts possess broad discretion in imposing conditions of supervised release.” *United States v. Betts*, 886 F.3d 198, 202 (2d Cir. 2018). A district court may impose special conditions of supervised release if they are “reasonably related” to the nature and circumstances of the offense, the history and characteristics of the defendant, the need for the sentence imposed to afford adequate deterrence to criminal conduct, the need to protect the public from further crimes of the defendant, and the need to provide the defendant with correctional treatment in the most effective manner. *United States v. Carlineo*, 998 F.3d 533, 536 (2d Cir. 2021) (citing U.S.S.G. § 5D1.3(b)).

Applying that standard here, the computer monitoring condition is warranted. The defendant committed complex cybercrimes, attempted to conceal them by using an alias, attempted to conceal or destroy a phone upon arrest, and continued to commit identity theft crimes even after he knew he was under federal investigation. Computer monitoring is thus “reasonably related” to (a) the circumstances of the offense—a complex cybercrime—and (b) the history and characteristics of the defendant and the need to protect the public from further crimes of the defendant—since Singh attempted to conceal or destroy evidence and continued to engage in criminal conduct after he was under investigation. Where, as here, the defendant is known to “erase or conceal” evidence, “a computer monitoring condition may be reasonably necessary for the purposes of sentencing.” *United States v. Pepio*, No. 23-6967-CR, 2024 WL 4929251, at *2 (2d Cir. Dec. 2, 2024). So too for a defendant who continues criminal activity after law enforcement contact. *See United States v. Savastio*, 777 F. App’x 4, 6 (2d Cir. 2019) (history of committing internet crime and prior violations of supervised release justified computer monitoring condition).⁶

⁵ To date, it appears that Victim-1 has not provided a loss affidavit to the Probation Department.

⁶ The defense errs in complaining that computer monitoring is not appropriate because this is not a sex offense case. Ltr. 2. While the Guidelines deem computer monitoring appropriate in sex offenses, they do not foreclose its imposition in other contexts. To the contrary, the prefatory section of the Guidelines cited by the defendant make clear that such special conditions, like monitoring, “may otherwise be appropriate in particular cases.” U.S.S.G. § 5D1.3(d). Indeed, the Court’s own guidance indicates that computer monitoring is appropriate in cybercrime cases. *See Overview of Probation and Supervised Release Conditions: Chapter 3:*

Last, the defense challenges a special condition for financial monitoring. Ltr. 3; PSR ¶ 98. The government agrees that the condition is not necessary under the circumstances.

V. The Section 3553(a) Factors Demand a Substantial Term of Incarceration

As explained in greater detail below, a substantial sentence of incarceration is warranted given the nature and seriousness of the defendant’s criminal offenses, the requirement to promote respect for the law, and the need for both general and specific deterrence. *See* 18 U.S.C. § 3553(a). For these reasons, the government respectfully submits that a Guidelines sentence of imprisonment of 30 to 36 months is sufficient, but not greater than necessary, to satisfy the goals of sentencing. *Id.*

A. Nature and Circumstances of the Offense

The defendant perpetrated a complex cybercrime and identity theft conspiracy that warrants a substantial penalty. His criminal conduct was serious in nature and broad in scope. Using his resources and contacts through his membership in the cybercriminal group “ViLE,” Singh inflicted substantial harm on various victims, including social media platform providers and federal law enforcement officers and agencies.

Singh also committed his crimes using sophisticated, malicious, and exploitative means. The defendant’s actions were deliberate—he exploited his access to personal victim information and confidential federal law enforcement intelligence. Singh harassed and extorted Victim-1, threatening to harm Victim-1’s parents. PSR ¶ 16. While the defendant argues that his youth is a mitigating factor, it is so only to a modest degree. This is because his crimes were not momentary lapses in judgment. Rather, the defendant—repeatedly and over a period of years—engaged in complex criminal activity. Nor do deaths in the defendant’s family, while tragic, explain or excuse his conduct. The passings predate his criminal conduct by several years.

Singh violated data privacy, undermined the integrity of highly confidential information, took advantage of custodians of private customer records, and compromised the security of a federal law enforcement database and highly sensitive intelligence materials. Data privacy impacts every citizen, agency, company, and institution in the United States. Social media platforms and providers, in particular, retain and safeguard a trove of private information that is not, and ought not to be, accessible to the public. A threat actor who knowingly penetrates these sensitive systems and databases, without authorization, poses a threat to any account holder, officer or otherwise. Similarly, the ability of law enforcement to confidentially and securely conduct criminal investigations and generate and store intelligence materials is of paramount importance.

Cybercrime-Related Conditions (describing computer monitoring options), <https://www.uscourts.gov/about-federal-courts/probation-and-pretrial-services/post-conviction-supervision/overview-probation-and-supervised-release-conditions/chapter-3-cybercrime-related-conditions-probation-and-supervised>.

B. General and Specific Deterrence

Given that criminal conduct like the defendant's is highly complex and typically difficult to detect and prosecute, principles of general deterrence warrant a substantial penalty. *See, e.g., Harmelin v. Michigan*, 501 U.S. 957, 988-89 (1991) (noting that “since deterrent effect depends not only upon the amount of the penalty but upon its certainty, crimes that are less grave but significantly more difficult to detect may warrant substantially higher penalties”). Because internet and fraud-based crimes are more rational, cool and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence. *See United States v. Zukerman*, 897 F.3d 423, 429 (2d Cir. 2018) (“Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it.”) (quoting *United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994)).

Here, a Guidelines sentence will help to deter Singh, other ViLE members, and cybercriminals at large, who believe that they can generate income through computer intrusion, identity theft, social engineering, and fraudulent schemes against data providers and law enforcement agencies. Such persons should know that deceiving data providers into handing over private subscriber information, penetrating law enforcement databases, and unlawfully intercepting government intelligence, will result in a substantial term of custody. In addition, the nature of cybercrime activity generally renders it more difficult to uncover: cybercriminals engaged in computer intrusion and identity theft often use their technological advantage and fluency in online systems to cover the tracks of their digital footprints, obfuscate their identities, and evade law enforcement detection, as Singh attempted here.

Additionally, computer intrusions, identity theft, and cyberattacks are prevalent and ever-growing. The Federal Bureau of Investigation's Internet Crime Complaint Center (“IC3”) has calculated that in 2024 alone, internet crimes exceeded \$16 billion in losses—a 33% increase in losses from the prior year.⁷ According to this same report, the top three most prevalent internet crimes of 2024 were email phishing, extortion, and personal data breach, all of which are relevant or directly applicable to ViLE's activities and Singh's specific conduct: namely, “doxing” as a form of extortion, and exploiting stolen credentials, respectively. *See id.* Additionally, according to IC3's report, identity theft, computer intrusion (or “hacking”) and government impersonation are also prevalent and responsible for substantial financial loss annually. *See id.* Identity theft and computer intrusion in particular permeate various kinds of cyberattacks and cyber-enabled financial fraud, including the crimes in question, and government impersonation is the means Ceraolo used to fraudulently issue a subpoena and obtain subscriber information.

⁷ *See* Fed. Bureau of Investigation, Internet Crime Complaint Ctr., 2024 IC3 Annual Report (2024), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (last visited May 16, 2025)

The defendant also needs to be specifically deterred. Singh was an active member of an advanced cybercrime group that is dedicated to illicitly obtaining victims' personal information and using that data to "dox" victims through exposing their personal data, until they pay or surrender property as ransom. ViLE hacked into law enforcement databases, deliberately accessed and stole sensitive personal information, and leveraged this information to control its victims through threats and harassment. Notably, Singh was not deterred by law enforcement executing a search at his home. He continued to engage in identity theft and attempted to conceal or destroy a phone. Accordingly, a Guidelines sentence would serve the interests of accountability, public safety, data privacy, and cybersecurity. Under these circumstances, the requested sentence is sufficient, but not greater than necessary, to achieve the goals of sentencing.

VI. Conclusion

For the reasons set forth above, the government respectfully requests that the Court impose a Guidelines sentence.

Respectfully submitted,

JOSEPH NOCELLA, JR.
United States Attorney

By: /s/
Alexander F. Mindlin
Ellen H. Sise
Adam Amir
Assistant U.S. Attorneys
(718) 254-7000

cc: Clerk of the Court (FB) (by ECF)
Defense Counsel of Record (by ECF and email)
U.S. Probation Officer (by email)